DoD Strategic Plan for Personnel Security[1]

Revised Draft December 14, 2000

Mission

The mission of the DoD personnel security program is to support DoD operations by ensuring that military, civilian, and contractor personnel assigned to and retained in positions in which they could potentially damage national security are reliable and trustworthy, and that there is no reasonable basis for doubting their allegiance to the United States.

Introduction

The disintegration of the USSR in 1991, and with it the abrupt end of the Cold War, caused dramatic changes in the environment in which Department of Defense (DoD) business is conducted. Diplomatic, economic, technological, political, and legal sectors have all been transformed. Combined with innovations in information technology and the global economy, these changes are a serious challenge to the DoD personnel security system, which dates from the early 1950s[2,3,4]. Numerous studies of the system over the past 15 years have pinpointed problems and recommended improvements. Although some recommendations have been undertaken, a major revision of the DoD personnel security system appears to be necessary. With the reality of a significant backlog of investigations, and resultant delays of a year or more in granting security clearances, the need for such a revision has become urgent. In the past the DoD has not had a strategic plan for personnel security. The following plan will serve as the basis for a major revision of the system.

Background. Recent global changes indicate that it is time for the DoD personnel security program to move away from the current monolithic approach to one that offers more flexibility. The end of bi-polar competition with the USSR does not imply that the threat is over and that personnel security budgets and staffs can safely be cut back. Security threats in the post-Cold War setting come not only from foreign intelligence services, but also from numerous and various sources including terrorist organizations, disaffected nations, militant religious groups, and potential economic competitors among others. Potential new threats, not yet fully understood- -for example, surreptitious attacks on a widespread and growing DoD information technology infrastructure—may now come from many sources. The need to respond to security threats is more complex and may, in fact, be greater than during the Cold War.

---

[1] This plan is based on input from participants at the DoD Strategic Planning Workshop on Personnel Security. 11/14/00-11/16/00, Monterey CA.

[2] Personnel Security Investigations Process Review Team reports on: "An Assessment of DoD's Plan to Eliminate the Periodic Reinvestigation (PR) Backlog" October 2000, and "An Assessment of the DoD Personnel Security Program", November 2000.

[3] Personnel Decisions Research Institute, Inc. (Bosshardt, M.J., Draft September, 2000). Issues in Developing a New Conceptual Framework for the DoD Personnel Security Program.

[4] FBI Director Louis Freeh, "Threats to U.S. National Security," Statement for the Record before the Senate Select Committee on Intelligence, January 28, 1998.

Since the end of the Cold War, several global trends have increased the need for a strategic plan and improved personnel security system (see Appendix A). These trends include global changes in computer technology and interchange that have increased DoD's vulnerability to, and risk of, insider betrayal. A global information explosion has compounded this vulnerability by increasing the varieties of information to protect. These trends exacerbate other DoD challenges—such as resource cuts, the development of some personnel security policies without full regard for their adverse impact on the system, and the lack of a centralized authority responsible for providing continuing evaluation—resulting in a DoD personnel security system that is overwhelmed.

Over recent years DoD has tried hard to meet these new challenges and to respond to ever more personnel security investigation (PSI) requests. Improvements that have been undertaken have been too piecemeal to achieve the desired effect. We see symptoms of crisis in the system now that point to the need for immediate and larger scale actions: 1) the current backlog of many thousands of new and periodic investigations, 2) delays in granting clearances that run from months into years, 3) lagging data collection and information management technologies that do not meet current standards for information systems, and 4) a lack of standardization, prioritization, and flexibility across the system that cannot be ignored. The need for a comprehensive strategic plan and coordinated action is urgent.

Moving Forward. To achieve major revisions in the personnel security program, the effort will require high-level visibility and consistent support from senior management in DoD. Because the post-Cold War environment and the global information age present new and different threats to the nation's interests if critical information were improperly disclosed, the personnel security system should be a primary concern of senior DoD officials who provide oversight, support, and the funding it needs to respond. This plan outlines the goals and objectives of a modernized, more flexible personnel security system, and makes specific recommendations for action. One important recommendation is to ensure continued, direct involvement by the Deputy Secretary of Defense (DepSecDef) as the senior official responsible for security in DoD. A senior-level panel, chaired by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD C3I), would be charged with implementing the strategic plan for personnel security and advising the DepSecDef on personnel security issues related to the Strategic Plan. This panel should include senior security officials of the military departments and the Joint Chiefs of Staff. The DepSecDef would receive quarterly updates of progress and an annual report on results, including recommendations for any mid-course corrections to the plan that may be necessary.

Finally, an effective program needs to be dynamic and able to adapt quickly to change. It is not enough to carry on blindly doing a given set of tasks—evaluation, and improvement based on that evaluation, should be built into the system. For example, the evolution of information technology is so rapid and unpredictable, that these seductive tools could threaten security in ways we cannot now imagine. This strategic plan relies on objective research and revisions to the system based on the findings of research to provide mechanisms for correction and improvement.

Personnel Security Goals, Objectives, and Action Items

GOAL 1. POLICY and OVERSIGHT: Effective and timely policy development and implementation, with active oversight by senior management.

Objectives

1.1: Compatibility between the DoD and DCI Personnel Security Strategic Plans.

1.2: Consistent and effective policy implementation.

1.3: Programs and proposals that include measures and the means to evaluate and monitor program effectiveness.

1.4: Policy formulation that is supported by research wherever feasible.

Action Items

1a: Designate the DepSecDef as the senior personnel security official for DoD.

1b: Designate responsible Component senior security officials to represent their agency in the prosecution of the strategic plan and to serve as advisors to the DepSecDef.

1c: Create and resource a senior oversight body.

1d: Report semi-annually to the senior oversight committee on progress in achieving strategic plan goals.

1e: Include DoD SOIC representatives and representatives of collateral clearance programs on policy boards to ensure compatibility with the DCI Personnel Security Strategic Plan.

1f: Encourage policy developers to identify long-term programmatic research needs.

1g: Review policy periodically for compliance with personnel security strategic goals.

1h: Identify and use "best practices" in the implementation of policy.

1i: Coordinate policy development among personnel security stakeholders.

1j: Convene periodic meetings to ensure effective policy communications.

GOAL 2. RESOURCES: Resource allocation that is integrated with personnel security policy development and implementation.

Objectives

2.1: Policy proposals and decisions that include considerations of cost impact.

2.2: Accurate resource requirements for the implementation of the personnel security program.

Action Items

2a: Develop a mechanism to estimate the baseline and continuing costs of personnel security across DoD.

2b: Define and identify resources associated with proposed policy and program implementation.

2c: Require that proposed policy and program changes that increase workload be appropriately resourced.

2d: Estimate the risks and costs of inadequate funding for proposed policy and program changes.

2e: Estimate the benefits of adequate funding, including direct benefits to security and indirect organizational benefits, e.g., lower turnover, for proposed policy and program changes.

GOAL 3. CLEARANCE REQUIREMENTS: Predictable clearance requirements that are tied directly to position risk factors.

Objectives

3.1: A flexible model for accurately predicting specific future requirements in the personnel security system for 1-5 years.

3.2: Position risk factors that are clear and specific.

3.3: Clearance requirements that are continuously evaluated.

Action Items

3a: Determine—define, develop, validate—investigative requirements for each military or civilian position, including positions open to contractors, on a periodic basis.

3b: Develop a predictive model for future investigative requirements and associated costs for 1-5 years.

GOAL 4. INVESTIGATIONS: Personnel security investigations that are timely, high quality, consistent, and in accordance with all applicable standards.

Objectives

4.1: Uniform standards for assessing timeliness and quality of investigations.

4.2: Standardized and integrated request procedures and input formats for all investigative providers.

4.3: Timely and effective management of investigative scope, especially in the area of overseas leads.

4.4: PSIs that are responsive to the needs of the DoD.

Action Items

4a: Identify and evaluate alternative business and information technology processes to the existing PSI system.

4b: Allocate investigative resources to cases by level of security risk.

4c: Create flexibility to fast-track high-priority requests for PSIs.

4d: Complete SSBIs in 90 days or less.

4e: Complete NACLCs in 60 days or less.

4f: Complete SSBI PRs in 120 days or less and Secret PRs in 60 days or less.

4g: Complete overseas leads in 90 days or less.

4h: Encourage uniformity and compatibility between the EPSQ/EQSP systems.

4i: Establish and encourage a 100% quality standard for investigative deliverables.

Goal 5. ADJUDICATIONS: Adjudications that are timely, high quality, and in accordance with all applicable standards.

Objectives

5.1: Uniform standards for assessing timeliness and quality of adjudications.

5.2: Judicious and limited use of interim SCI access.

5.3: Reciprocity among DoD agencies for personnel with security clearances.

5.4: Fairness and accountability of the appeal process.

Action Items

5a: Complete clearance determinations in an average of 30 days or less.

5b: Develop a standardized electronic reporting format that describes the rationales for favorable and unfavorable decisions.

5c: Train the adjudicative and investigative communities in how to identify CI indicators.

5d: Incorporate CI reviews in appropriate adjudications.

5e: Identify options for improved adjudicative processes and how such processes might function.

5f: Conduct a-periodic program assessments by an interagency review team.

GOAL 6. CONTINUING EVALUATION: A proactive continuing evaluation program.

Objectives

6.1: Evaluations of cleared employees, based on programmatic research, that incorporate weighted risk factors, sensitivity of position, periodicity, and scope.

6.2: Effective integration and use of automated systems and electronic databases.

6.3: Integration of evaluation programs with disciplines that impact personnel security, e.g., EAP, CI, human resources.

6.4: High deterrent impact of continuing evaluation.

Action Items

6a: Define PR risk factors and sensitivity levels.

6b: Revise PR periodicity and scope.

6c: Test and evaluate automated evaluation systems.

6d: Draft, coordinate and implement policy initiatives to encourage greater use of self-help resources, such as private counseling, employee assistance programs, or financial counseling.

6e: Incorporate continuing evaluation into management training, and get management support and involvement.

6f: Clearly identify reporting channels and responsibilities.

GOAL 7. SECURITY AWARENESS: Effective security awareness and compliance at all levels within DoD.

Objectives

7.1: Comprehensive reporting of, and attention to, improper, unreliable, or suspicious behavior and related conditions.

7.2: Integration of current and relevant counterintelligence threat information into security awareness programs.

7.3: Management accountability for security awareness.

7.4: Individual accountability for security awareness.

Action Items

7a: Increase the use of flexible automated systems, such as the "Customizable Employee's Guide to Security Responsibilities," for making security awareness information readily available on the computer desktops of personnel and managers.

7b: Include security awareness and compliance goals in individual performance plans.

GOAL 8. SENSITIVE BUT UNCLASSIFIED INFORMATION AND ENVIRONMENTS: **Effective risk management of individuals with sensitive duties but no access to classified information, especially information technology personnel with access to high risk data and information systems.**

Objective

8.1: Appropriate investigations and adjudications for individuals with sensitive duties but no access to classified information.

Action Items

8a: Develop a model to assist with the categorization of risk for sensitive but unclassified information.

8b: Develop appropriate standards and procedures for investigation and adjudication of individuals with sensitive duties but no access to classified information.

8c: Define the applicable population and positions, as well as a mechanism to estimate annually the type and total of investigative requirements in this area.

8d: Identify the organization(s) responsible for monitoring and managing programs for personnel with access to sensitive but unclassified information.

GOAL 9. TRAINING AND PROFESSIONAL DEVELOPMENT: **Comprehensive recruitment, training, education, and professional development of security personnel, along with appropriate infrastructure.**

Objectives

9.1: Recruitment and retention of quality personnel with diverse skills.

9.2: Certification of security professionals to high, consistent standards.

9.3: Broad and efficient access to reports, data, and knowledge by relevant groups in the personnel security community.

9.4: Effective and proactive management of projected attrition of the professional security workforce.

Action Items

9a: Establish a military specialty for security professionals.

9b: Develop a professional career path for security professionals.

9c: Develop a plan in coordination with Human Resources to institute a "best practices" recruitment, retention, and professional development strategy.

9d: Expand the capability and use of a centralized DoD security training facility, such as the DSS Academy, for security professionals.

GOAL 10. RESEARCH: A personnel security research capability in support of DoD and national security strategic priorities.

Objectives

10.1: Ongoing personnel security research based on a strategic plan, DoD requirements, and "buy in" (coordination and cooperation) across the community.

10.2: Long-term programmatic research on personnel security programs.

10.3: Quick-response capability for research issues that need fast attention.

10.4: Efficient dissemination and accessibility of research results across the community.

Action Items

10a: Ensure the capability to develop research products that meet the needs of the community.

10b: Ensure the capability to conduct research that meets emerging needs.

10c: Reestablish a DoD research advisory/oversight group and encourage all stakeholders to participate.

10d: Explore and incorporate appropriate non-DoD personnel security research.

10e: Disseminate research across DoD and intelligence communities.

10f: Publicize the DTIC (Defense Technical Information Center) among personnel security stakeholders to facilitate the dissemination of research.

Appendix A
Recent Trends in the Personnel Security Environment

The task of ensuring the loyalty, reliability, and trustworthiness of the cleared workforce is now more difficult and complex due to the end of the Cold War paradigm in international relations and the revolution in information technology over the past 20 years. The personnel security system is at the very heart of the government's security system and will remain the centerpiece of the Federal security system in the post-Cold War era[5]. DoD's need for a different kind of personnel security system arises, in part, from these recent changes. For example, in this new environment, the amount of information that can be compromised by a single insider working for a foreign intelligence service has increased substantially. The requirement to protect a new category of material, sensitive but unclassified information, means that more people are in a position to damage national security. Faced with these new challenges, along with rapid growth in the number of clearance requests, the current DoD personnel security system has become overloaded, technologically outdated, under-funded, and showing signs of breakdown.

Computer Technology: Increased Vulnerability to Insider Betrayal. Computers concentrate vast amounts of data in one location, where it is vulnerable to unauthorized or accidental disclosure, modification, or destruction. The greater the concentration of data, the greater the potential and consequences of a security breach. Reliance on networked computer databases, designed to improve information sharing, has also increased the scope of damage that a single insider can do. Computer networks solve the spy's age-old dilemma—how to obtain the precise information that is most valuable to a foreign buyer. The equivalent of safe-loads of classified material can now be copied in minutes and immediately transmitted around the globe, often with little risk of detection. How different this is from the days when classified information on paper was stored in safes to which a handful of people had access, and when spies incurred significant risk in transmitting even small amounts of information to their foreign handlers. As more people have access to more information through networked computers, the opportunity to commit espionage is likely to increase.

Global Interchange: Increased Risk of Insider Betrayal. During the past 20 years, roughly four-fifths of Americans arrested for espionage had volunteered their services to another country, although one-quarter of those were caught before they could pass on any classified material.[6] In the current global economy in which our country is the only superpower, there are many countries engaged in espionage against the United States. It is now easier than ever for Americans who contemplate volunteering information or material to initiate contact with a foreign intelligence service. Foreign intelligence collectors likewise take advantage of these circumstances to spot, assess, and then manipulate or recruit unsuspecting Americans with access to classified, controlled, or proprietary information. The global interchange characteristic of our era allows collectors to develop frequent, casual contact with Americans who may have access to classified information and who have legitimate business contacts with representatives from many countries. Under these circumstances, volunteer spies are less vulnerable to detection by the counterintelligence screens that have been successful in the past.

---

[5] Chapter 4, Joint Security Commission I, February 28, 1994.

[6] Espionage database maintained by Defense Personnel Security Research Center.

In high technology fields, practitioners routinely come from many different countries. Combined with the variety of countries now conducting intelligence operations against the United States, this international trend generates conflicting loyalties. About half of all the doctoral degrees in physics, chemistry, and computer science granted by U.S. universities now go to foreign-born students.[7] Approximately one-third of all the engineers in Silicon Valley are foreign born.[8] Of Americans prosecuted for espionage between 1940 and 2000, 18 percent were naturalized citizens. This is appreciably larger than the 3.5 percent of the national population, or the 3.4 percent of DoD clearance holders, who are naturalized citizens.[9] In addition, job-hopping is now routine for certain types of professionals. These shifts to routine global contacts, an international viewpoint, and higher employee turnover have put new strains on the task of assessing and ensuring loyalty.

As allies and presumed friends target US technology for intelligence collection, the distinction between friend and foe is weakened. Offers of information to allies in recent espionage cases reflect this weakening. The current climate makes it easier for an American to rationalize passing protected information to a foreign power as "just a business proposition," rather than a heinous activity that puts the security and survival of the country at risk.

Information Explosion: Increased Varieties of Information to Protect. As the Internet and networked computer systems change the handling of information, the distinction between classified and unclassified information is blurred. Ironically, at a time when significant efforts are being made to reduce the amount information that is classified, the quantity of sensitive but unclassified information (both government and proprietary) that requires some form of control or protection has grown substantially. The number of people with access to this sensitive information has increased accordingly. Automated information systems are creating a new class of personnel—information systems professionals—who are of concern to the personnel security system even when they do not have access to classified information. For example, information systems analysts have insider access to logistics, personnel, financial, communications, and other unclassified systems. Consequently, these information professionals are in a position to compromise, modify, or destroy systems that, though unclassified, are essential to military operations.

In the defense industry, many more people—for example, engineers, and information systems professionals as well as maintenance staff, temporary employees, and guards—now have access to sensitive but unclassified technical and scientific data relating, in particular, to US weapons systems. This is due, in part, to changes in DoD acquisition policy, which now encourages the integration of the defense industrial base with the commercial industrial base. Most militarily critical technologies are now dual-use technologies, that is, the same technology has both military and civilian applications. Consequently, the loss of this unclassified but proprietary or embargoed technology may damage military security as well as the economy. In a

---

[7] National Academy of Sciences (1995). *Reshaping the Graduate Education of Scientists and Engineers.* National Academy Press, p. 70.

[8] Gilder, George (1995, Dec. 18) "Geniuses from Abroad," *Wall Street Journal.*

[9] Espionage database maintained by Defense Personnel Security Research Center. Susan M. Hagan & Martin F. Wiskoff, *Espionage by U.S. Citizens: 1940 – 2000.* Paper presented at 41st Annual International Military Testing Association Conference, November 10, 1999.

world that increasingly measures national power and national security in economic terms, foreign countries and corporations are placing increased emphasis on the collection of scientific, technical, and economic information of all types.

The risks associated with these recent trends are clear. The need for action is urgent.